

TASK ORDER (TO)

47QFCA19F0033

Cyberspace Operations Support

in support of:

Army Cyber Command (ARCYBER)



Issued to:

**Perspecta Engineering, Inc
15050 Conference Center Dr.
Chantilly, VA 20151**

Awarded by:

**The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405**

**Awarded: 14 December 2018
Modification PS01**

FEDSIM Project Number 2017094AR

C.1 BACKGROUND

United States (U.S.) Army Cyber Command's (ARCYBER) mission is to direct and conduct integrated Electronic Warfare (EW), Information Operations (IO), and Cyberspace Operations, as authorized or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to adversaries. Established in October 2010, ARCYBER is the Army Service Component Command (ASCC) to the U.S. Cyber Command (USCYBERCOM), responsible for conducting cyberspace operations (i.e., Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and Department of Defense Information Network (DODIN) operations), as directed and authorized, on behalf of Commander, USCYBERCOM. ARCYBER organizes, trains, educates, mans, equips, funds, administers, deploys, and sustains ARCYBER forces to conduct cyberspace operations.

Successful execution of ARCYBER cyberspace operations requires integrated and synchronized OCO, DCO, and DODIN operations. ARCYBER is currently comprised of a Contractor, Civilian, and Military workforce working together to execute its mission. Historically, operational barriers have existed, such as, organizational silos and contractual constraints, that could be resolved with a fully integrated enterprise operations solution. Moreover, the cyberspace battlefield has created the demand for an instrument that can rapidly deploy cyber resources and capabilities on a near, real-time basis in order to contend with the adversary. These challenges create the vision for the Cyberspace Enterprise Operations TO.

In addition, Army plans to improve readiness and integration through the consolidation of its core mission functions at one strategic location in Fort Gordon, Georgia (GA). Along with co-locating functions, this major relocation from Fort Belvoir, Virginia (VA) will also enhance mission partnerships with the Cyber Center of Excellence (CCoE) and the National Security Agency (NSA). The transition is currently projected to begin as early as Fiscal Year (FY) 2020 and be completed No Later Than (NLT) the Fourth Quarter (4Q) in FY22. However, the exact timeframe hinges on the completion of the new facility at Fort Gordon, GA. This relocation will require close coordination with the Cyberspace Enterprise Operations support contractor. Contractor support shall serve in a capacity that ensures no degradation of services during the transition.

The essence of this TO is to close the business, operations, mission resource, and capability gaps and provide continuity for the primary ARCYBER Headquarters (HQ) and Joint Force Headquarters – Cyber (JFHQ-C), ARCYBER subordinate units, and DOD partnering organizations.

C.2 SCOPE

The scope of this TO is to provide cyberspace operations support for ARCYBER HQ, JFHQ-C, ARCYBER subordinate components, service component partners of CYBERCOM, and other DOD cyber mission partners. The scope of this support includes program management; intelligence support; DCO; endpoint security; information assurance; DODIN operations; protection programs; plans and policy support; training and exercise support; IO; communications support; and force development.

In addition, ancillary services will be provided under this TO as required. Travel in the Contiguous United States (CONUS) and OCONUS travel will be required.

C.3 CURRENT ENVIRONMENT

The Army Cyberspace Command and Control (C2) Framework in Attachment T of the TO provides a depiction of the current operational environment and Command relationships necessary to carry out missions.

C.4 OBJECTIVE

The objective of this TO is to enable the advancement and development of cyberspace operations support.

C.5 TASKS

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site: the Enterprise Contractor Manpower Reporting Application (ECMRA). The contractor shall completely fill in all required data fields using the following web address:
<http://www.ecmra.mil/>.

Reporting inputs will be for the labor executed during the period of performance during each Government FY, which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported NLT October 31 of each calendar year. Contractors may direct questions to the support desk at: <http://www.ecmra.mil/>.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure website without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (**Section F, Deliverable 1.0**). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM Contracting Officer's Representative (COR).

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 1.1**) for review and approval by the FEDSIM COR and the ARCYBER Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

- a. Points of Contact (POCs) for all parties.
- b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
- c. Staffing Plan and status of hiring activities.
- d. Transition-In Plan and discussion.
- e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
- f. Invoicing requirements.

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (**Section F, Deliverable 1.2**) within three workdays following the Kick-Off meeting. The report shall document the Kick-Off Meeting discussion and capture any action items.

C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (**Section J, Attachment F**) (**Section F, Deliverable 1.3**) covering all activities performed under the TO. The MSR shall include the following:

- a. Activities during reporting period (include on-going activities, new activities, and activities completed, and progress to date on all above mentioned activities). The format of the report and presentation shall be organized by task area and/or section and each shall start with a brief description of the activities performed within the month.
- b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- c. Personnel gains, losses, and status (security clearance, etc.).
- d. Government actions required.
- e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- f. Cost incurred for each CLIN up to the previous month.
- g. Projected cost of each CLIN for the current month.

C.5.1.4 SUBTASK 4 – CONVENE MONTHLY TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting with the assigned TPOC, FEDSIM COR, and other Government stakeholders (**Section F, Deliverable 1.4**). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of

these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the TPOC and FEDSIM COR within five workdays following the meeting (**Section F, Deliverable 1.5**).

C.5.1.5 SUBTASK 5 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (**Section F, Deliverable 1.6**) on which the Government will make comments. The final PMP (**Section F, Deliverable 1.7**) shall incorporate the Government's comments.

The PMP shall:

- a. Describe the proposed management approach.
- b. Include project/work request milestones, deliverables, tasks, and subtasks.
- c. Contain detailed Standard Operating Procedures (SOPs) for all applicable project/work requests.
- d. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.

C.5.1.6 SUBTASK 6 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated as the project changes (annually at a minimum) (**Section F, Deliverable 1.8**). The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (**Section F, Deliverable 1.9**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in **Section J, Attachment G**.

C.5.1.8 SUBTASK 8 – COLLABORATIVE WORKING GROUP

The contractor shall establish a collaborative working group to share information such as subject matter expertise, best practices and lessons learned, and process and procedure gaps and recommended improvements. The contractor shall identify key group members and ensure participation in a periodic working group (**Section F, Deliverable 1.10**). The contractor shall create an agenda, develop working group topics, and schedule and coordinate meeting locations. The contractor shall ensure participants have an understanding of the purpose and intent of the working group prior to each meeting. The contractor shall conduct working group sessions and document feedback and recommendations for Government review (**Section F, Deliverable 1.11**). The contractor shall use the working group to develop recommendations that improve the efficiency and effectiveness of mission execution (**Section F, Deliverable 1.12**).

C.5.1.9 SUBTASK 9 – CONTINUITY OF OPERATIONS (COOP) SUPPORT

The contractor shall provide COOP-related support within the capabilities of the TO to ensure the continuation of services and essential functions across a wide range of emergencies and events. Execution of COOP-related support requirements cover the range of planning, mitigation, response, and recovery actions needed to maintain the continuity of operations provided capabilities. COOP plans shall utilize current and subsequent policies and publications (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev. 1). COOP support shall include COOP plans, procedures, tests, training, and exercises essential for ensuring a viable COOP capability. This shall include, but is not limited to, the following activities:

- a. Develop emergency preparedness plans and procedures (**Section F, Deliverable 1.16**) that delineate Mission Effectiveness Functions (MEFs) to include Mitigation and the Devolution and Reconstitution of MEFs.
- b. Ensure safekeeping and accessibility of vital records, files, and databases needed to support essential functions.
- c. Provide alternate communications that enable the enterprise to perform essential functions, in conjunction with mission partners, until normal operations can be resumed.
- d. Provide continuity awareness training for the execution of COOP and related contingency plans.
- e. Ensure that the COOP program is capable of supporting the continued execution of its essential functions throughout the duration of a COOP situation (as defined by a level of effectiveness measured over a period of time and by type of scenario). At a minimum, the contractor shall conduct table top exercises quarterly and full COOP exercises annually (**Section F, Deliverable 1.17**).

C.5.1.10 SUBTASK 10 – TRANSITION-IN

The contractor shall provide a 60-day seamless transition from the incumbent(s) and ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor may be required to coordinate with multiple incumbent contractors during transition. Ten workdays after the kick-off meeting, the contractor shall update the draft Transition-In Plan provided with its proposal and provide a final Transition-In Plan as required in Section F (**Section F, Deliverable 1.13**). The final Transition-In Plan shall include all applicable services identified by the Government to be transitioned in the 60-day transition-in period. The contractor shall implement its Transition-In Plan NLT 60 calendar days after award and all transition activities shall be completed after approval of the final Transition-In Plan.

C.5.1.11 SUBTASK 11 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (**Section F, Deliverable 1.14**). The Government will work with the contractor to finalize the

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

Transition-Out Plan (**Section F, Deliverable 1.15**) in accordance with Section E. The Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- a. Project management processes.
- b. POCs.
- c. Location of technical and project management documentation.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor to contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel.
- g. Schedules and milestones.
- h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.1.12 SUBTASK 12 – RELOCATION MANAGEMENT TO FORT GORDON

The contractor shall manage the relocation of all TO functions performed at a Fort Belvoir, Virginia (VA) duty station to the new ARCYBER facility located in Fort Gordon, GA. Relocation shall be conducted in accordance with ARCYBER directives, policies, and plans. Advanced notification will be provided to the contractor with specific details on the relocation plan.

The contractor shall maintain appropriate service levels and ensure no disruption or service degradation during the relocation. Where possible, the contractor shall proactively develop solutions to address the relocation. The contractor shall provide a written plan for relocating functions under the TO and present information as required (**Section F, Deliverable 1.18**). The contractor shall maintain close coordination with the Government to include providing progress/status updates on relocation activities (**Section F, Deliverable 1.19**), as required.

C.5.2 TASK 2 – SECURITY OPERATIONS

The contractor shall provide operational security support. Contractor support shall include, but is not limited to, the following activities:

- a. Assist in the administration, operations, and maintenance of a special security program/office.
- b. Develop, evaluate, and maintain the operational plans, policies, devices, procedures, and methods used for safeguarding classified information, property, and materials (**Section F, Deliverable 0.8**).
- c. Assist in the analysis and evaluation of personnel responsible for accessing classified or sensitive information, materials, or work sites.

- d. Maintain control and accountability of classified materials (**Section F, Deliverable 2.0**) (e.g., North Atlantic Treaty Organization (NATO), Special Access Program (SAP), etc.) including the proper storage, transmittal, and/or destruction of materials.
- e. Provide guidance, training, instruction, and review on the handling of classified information by personnel and security awareness issues (**Section F, Deliverable 2.1**).
- f. Provide subject matter expertise on the accreditation, upgrades, and certifications of Sensitive Compartmented Information Facility (SCIF) related construction and equipment matters.
- g. Maintain the body of knowledge for all applicable security and Sensitive Compartmented Information (SCI) related directives, regulations, manuals, and guidelines for the program office (**Section F, Deliverable 2.2**).
- h. Develop and conduct briefings for senior military and civilian leadership (**Section F, Deliverable 0.3**).

C.5.3 TASK 3 – INTELLIGENCE SUPPORT

The contractor shall provide a full range of intelligence support capabilities that improve the full spectrum of global operations in the cyberspace domain. The range of intelligence capabilities provided shall assist the organization in collecting, analyzing, and disseminating actionable information through the development of various intelligence reports and products (**Section F, Deliverable 3.0**) as detailed throughout the subtasks. The contractor shall support the coordination, and execution of intelligence requirements across multiple intelligence disciplines within the organization and support the synchronization of intelligence with strategic partners (e.g., USCYBERCOM, Intelligence Community (IC), etc.). The activities performed in support of this task shall enhance situational awareness, enable rapid decision-making, and support current and long-term operational planning.

The contractor shall perform all services during the core operational hours or as required per the shift assignments and threat priorities. The contractor shall ensure shift change briefings (**Section F, Deliverable 3.1**) are conducted and adequate coverage is identified (**Section F, Deliverable 3.2**). The contractor shall conduct briefings for senior military and civilian leadership (**Section F, Deliverable 0.3**) as required.

C.5.3.1 SUBTASK 1 – INTELLIGENCE OPERATIONS

The contractor shall provide all-source intelligence analysis and production support for cyber threat warnings and notification (i.e., Indications and Warnings (I&W)) to networks, first phase analysis of cyber incidents, synchronization of the organization and cyber IC analytic efforts, and integration of intelligence support to the organization's DCO. The contractor shall provide intelligence support to DCO and across theaters of operation and interfaces with Joint, Sister Service, and Combatant Command (CCMD) operation centers. The contractor shall ensure intelligence personnel are trained in the execution of intelligence policies, processes, systems, and tools. The contractor shall follow applicable intelligence cycle and intelligence doctrine (e.g. DOD Joint Publications).

C.5.3.1.1 OPERATIONAL INTELLIGENCE SUPPORT

The contractor shall provide operational intelligence support using all-source analysis and methods to enhance situational understanding and awareness of cyberspace operations.

Contractor support shall include, but is not limited to, the following activities:

- a. Provide an intelligence support capability 24 hours per day, seven days per week, and 365 days per year (24x7x365), as required, for military cyberspace operations.
- b. Develop intelligence products for anticipated or unspecified intelligence production requirements.
- c. Support current and long-term planning for Cyber Intelligence Preparation of the Environment (CIPE) and Course of Action (COA) development.
- d. Participate in exchanges with partners, develop contacts with counterparts, establish analytic collaboration (i.e., subordinate units, higher agencies, the IC, and external partners) to maintain situational awareness to support services and joint common operations and to conduct intelligence and for information sharing.
- e. Maintain continuity of cyber threat individuals, cyber-personas, and organizations to support attribution and predict adversary COA.
- f. Conduct social network analysis of threat entities to facilitate order of battle and template creation.
- g. Conduct human factor and organizational analysis on cyber threat entities.
- h. Assist in the training of Field Support Team (FST) members prior to deployment, maintain contact, and provide support once deployed.
- i. Update appropriate databases and repositories for sharing and cataloging intelligence information.
- j. Develop Cyber Threat Reporting for events, as required.
- k. Develop and maintain Threat Briefing Assessments at the Unclassified/For Official Use Only (U/FOUO), SECRET, and Top Secret (TS) Level that reflect the current state of cyber threat activity with an emphasis on impact to the agency.
- l. Provide support to analysis of cyberspace operations TTPs development.
- m. Capture all analysis and technical details pertaining to adversary actions within the appropriate analytic repository.
- n. Identify intelligence gaps, develop intelligence requirements, and advocate those requirements during battle rhythm events for collection.

C.5.3.1.2 INDICATIONS AND WARNINGS (I&W)

The contractor shall provide I&W support to cyberspace operations, including contingency operations and exercises; research, analyze, and create products/reports from multiple intelligence and operational sources to provide situational awareness of critical elements of the cyber environment necessary to defend networks and the DODIN. Contractor support shall include, but is not limited to, the following activities:

- a. Provide a 24x7x365 I&W support capability as required for military cyberspace operations.
- b. Report I&W of malicious cyber activities.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- c. Provide crisis response and mitigation techniques to deny exploitation by the adversary; and, synchronize and integrate intelligence activities in order to detect, analyze, and recommend mitigation of cyber threats and vulnerabilities.
- d. Participate in exchanges with subordinate and higher agencies to maintain and provide situational awareness through deliverable products and reporting to facilitate decision making and intelligence driven operations.
- e. Perform technical analysis of computer network intrusion events and malicious activity in support of cyber intelligence efforts.
- f. Analyze trends and statistics of cyber activity to provide proactive I&W of malicious cyber activity throughout the DODIN that are affecting, or may affect, applicable networks in the future.
- g. Perform filter queries of network flow data and analyze results for anomalies and malicious indicators.
- h. Analyze the origins, pathways, and methodologies of malicious cyber activities to attribute, model, and predict future intrusions.
- i. Analyze computer network intrusion events and malicious activity to support intrusion detection and cyber-attack warning.
- j. Provide crisis response and mitigation techniques to deny further exploitation by the adversary; and, synchronize and integrate intelligence activities in order to detect, analyze, and recommend mitigation of cyber threats and vulnerabilities.
- k. Provide forensic analysis of captured packets, hard drive images, system logs, and sensor data used in all-source intelligence products.
- l. Provide recommendations for appropriate response and actions to the activity in order to identify vulnerabilities, correct faults, and defeat or defend against threat activity.
- m. Capture all analysis and technical details pertaining to adversary actions within the analytic repository.
- n. Report I&W of malicious cyber activities.

C.5.3.2 SUBTASK 2 – ANALYSIS AND CONTROL ELEMENT (ACE)

The contractor shall provide support to the ACE in developing forward-leaning intelligence products that enable rapid decision-making and drive operational planning to deliver timely effects in support of command priorities. ACE support shall include, but is not limited to, the following activities:

- a. Provide tailored, all-source current analysis addressing foreign and domestic Information Warfare and Computer Network Operations (CNO) capabilities, intentions, and actions affecting Army networks worldwide.
- b. Conduct research, analyze, and create products/reports from multiple intelligence and operational sources to provide situational awareness of critical elements of the cyber environment necessary to defend the network and DODIN.
- c. Monitor current activity trends of the organization's network and other Government and commercial networks.
- d. Contribute to the body of knowledge on foreign and domestic cyber capabilities and intentions.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- e. Develop a priority list of high profile personnel and groups to track including all named activities as well as other people/groups of interest.
- f. Assess threat modus-operandi, tools, techniques, alliances, and activities of hacker groups or cyber-related organizations and personnel within foreign governments, and of non-state actors such as terrorist groups. Describe the motivations and Command and Control (C2) structures of these people/groups, as appropriate.
- g. Support Requirements Management (RM) to track intelligence requirements and production efforts.
- h. Track and database all deliverables, Requests for Information (RFIs), and tasking for the section.
- i. Maintain records of all relevant cyberspace operations reports and task assignments for tracking purposes.
- j. Respond to RFIs related to developing new assessments, distributing established assessments, or briefing new/established assessments about cyber threat capabilities and intentions.
- k. Report and present analytical findings and conclusions.
- l. Fuse available intelligence with operational data into Signals Intelligence (SIGINT), if applicable, and Collateral Daily/Weekly Intelligence Summaries (INTSUMs).
- m. Create link analysis charts to visualize all reportable cyber activity and to track the scope and details of related activities.
- n. Update, maintain, and ensure Quality Control (QC) of appropriate classified databases and repositories.
- o. Review the data going into applicable databases for QC purposes and provide written feedback on any issues.
- p. Populate and update appropriate national and local databases and web pages.
- q. Identify and maintain a list of appropriate POCs at each organization that has a cyberspace mission including, but not limited to, Joint and Allied Task Forces, National IC, Law Enforcement and Counterintelligence (LE and CI) agencies, and other service CNO intelligence organizations.

C.5.3.3 SUBTASK 3 – TARGET SUPPORT

Target Support provides tactical intelligence analysis in support of threat mitigation activities. The contractor shall provide target support to cyberspace operations including contingency operations and exercises. Target support includes, but is not limited to, the following activities:

- a. Develop and produce intelligence, meaningful conclusions, and concise estimates of target activities and areas of interest to include target systems analysis reporting and electronic target folder development.
- b. Conduct liaison effort with other intelligence agencies and operational forces in support of target support operations.
- c. Develop and maintain communications and interface for intelligence and analytic matters dealing with assigned geographic areas within the global cyberspace domain.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- d. Prepare intelligence reports and present briefings on assigned Area of Responsibility (AOR) analysis to support the target nomination process in support of full spectrum cyberspace operations.
- e. Build and maintain intelligence electronic target folders to support target nomination.
- f. Conduct all-source intelligence analysis and assessments that supports target systems analysis.
- g. Research, evaluate, analyze, integrate, and interpret information from multiple intelligence and operational sources and fuse into finished target development products for anticipated or unspecified intelligence production requirements.
- h. Build and maintain threat target support data.
- i. Develop reports and products, both current and long-term, in support of planning Intelligence Preparation of the Battlefield (IPB) and COA development.
- j. Conduct the collection, interpretation, evaluation, integration, production, and dissemination of analytical products in response to the intelligence needs of the organization.
- k. Provide intelligence planning support to target development through the management of target development efforts associated with deliberate operational planning.
- l. Coordinate target intelligence support products across the IC for exercises in all geographic CCMDs.

C.5.3.4 SUBTASK 4 – JOINT INTELLIGENCE SUPPORT ELEMENT (JISE)

The contractor shall provide intelligence support for joint operations and exercises including security cooperation events. The contractor shall provide intelligence collection, production, analysis, and dissemination for joint forces (e.g., CCMDs). JISE support shall include, but is not limited to, the following activities:

- a. Develop and maintain a running intelligence estimate and common intelligence picture (CIP) synchronized with the common operations picture (COP) to enable the planning and execution of full-spectrum cyberspace operations.
- b. Produce daily, weekly, and monthly INTSUMs, as required.
- c. Conduct exchanges with IC partners and operational joint forces to maintain communications and situational awareness of daily activities within assigned AORs.
- d. Support Operational Planning Teams (OPTs) and Cyber Combat Mission Force (CCMF) by providing timely and accurate fused intelligence and doctrinal intelligence products containing meaningful assessments and concise estimates to include IPB, CIPE, and Enemy COAs.
- e. Collaborate with the internal partners (e.g., G2, ACE, and Combat Mission Team (CMT)) for fusion elements on production to answer command Priority Intelligence Requirements (PIR) and fill identified intelligence gaps organically.
- f. Interface with IC and Defense Intelligence Analysis Program (DIAP) partners to coordinate federation of requirements to fill intelligence gaps while collaborating internally to fulfill DIAP production responsibilities.
- g. Write source directed requirements, RFIs, and evaluations and/or feedback for serialized reporting and finished intelligence products with JFHQ-C equities in order to influence

the reporting and production cycle to address command PIR and fill gaps that cannot be answered organically.

- h. Write JFHQ-C Essential Elements of Information (EEIs) as input to National SIGINT information needs levied by partners across the intelligence community.
- i. Contribute to National Human Intelligence (HUMINT) collection directives and develop or provide input to enterprise-wide HUMINT collection requirements, as appropriate.
- j. Conduct gathering, interpretation, evaluation, integration, production, and dissemination of analytical products in support of the intelligence needs.
- k. Prepare and present intelligence briefings in support of Commander Update Briefs (CUBs) and the Military Operational Planning Process (MOPP)
- l. Provide all-source intelligence support to the planning and execution of exercises to include analysis and production for scenario development and road to war briefings, and active participation in exercises.

C.5.3.5 SUBTASK 5 – SINGLE SOURCE COLLECTIONS AND ANALYSIS SUPPORT

C.5.3.5.1 OPEN SOURCE INTELLIGENCE (OSINT)

The contractor shall provide OSINT collection, analysis, production, and dissemination of publically available information to enable situational understanding of cyberspace threats to networks and equities. OSINT support shall include, but is not limited to, the following activities:

- a. Develop and maintain a running intelligence estimate and CIP synchronized with the common operations picture to enable the planning and execution of full-spectrum cyberspace operations.
- b. Conduct OSINT research and queries in target language and English. Translate multimedia (e.g., audio and text) products from target language into English. Contractor personnel providing OSINT support shall have a language proficiency of 3 (ILR 3+/3+) in listening and reading as scored by the Defense Language Proficiency Test in the target language.
- c. Write intelligence reports and products in accordance with Intelligence Community Directive (ICD) 206 standards.
- d. Apply OSINT tradecraft to mitigate attribution and analysis to complex problems.
- e. Develop strategies to satisfy collection management OSINT tasking.

C.5.3.5.2 SIGNALS INTELLIGENCE (SIGINT)

The contractor shall provide SIGINT collection, analysis, production, and dissemination of SIGINT to enable situational understanding of cyberspace threats to networks and equities. SIGINT support shall include, but is not limited to, the following activities:

- a. Monitor and develop target sets across multiple communications technologies.
- b. Independently task across all authorities, maintaining compliance, without releaser, oversight officer, or legal rejection/modification.
- c. Build analytics for more complex discovery and analysis tasks.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- d. Understand multiple Internet Protocols (IPs), telecommunications technologies, and internet routing.
- e. Understand multiple communications protocols and analyze technical data from collected information for new collection opportunities.
- f. Identify information for signs of communications changes and identify alternate means of communication.
- g. Run complex queries using a variety of different tools.
- h. Provide support to aid in the creation/development of queries.
- i. Leverage new collection resources and share information with the Government and IC .
- j. Review information from streams of data to identify leads or complementing data to enhance overall analysis.
- k. Perform Dialed Number Recognition (DNR) and Digital Network Intelligence (DNI) development analysis.
- l. Work with other Signals Intelligence Development (SIGDEV) elements to introduce new tools/avenues of pursuit in an effort to find new collection.
- m. Discover alternate means of communication for complex and operationally sophisticated targets.
- n. Evaluate leads for tasking and use appropriate tasking authorities and assist in the creation of collection plans and prioritization.
- o. Advise key military, Government, and contract stakeholders on operational workflows and requirements.
- p. Process and develop SIGINT Geospatial information across DNI and DNR disciplines and recognize the convergence of circuit-based and packet-based telephony, and the increased emphasis on development of internet-based tasking and targeting.
- q. Develop strategies to satisfy collection management SIGINT tasking.

C.5.3.6 SUBTASK 6 – G2X SUPPORT

The contractor shall provide advanced intelligence support and operations in support of G2X mission requirements. G2X support is primarily conducted in support of ARCYBER HQ requirements and in conjunction with counterpart agencies, such as USCYBERCOM. The contract G2X support shall include, but is not limited to, the following activities:

- a. Perform coordination and communication of HUMINT and CI activities.
- b. Conduct research and analysis to support debriefing plans and question sets.
- c. Develop debriefing plans and question sets (e.g., incorporating biographical data).
- d. Support Key Leader Engagement (KLE) activities and briefings.
- e. Develop intelligence reports (e.g., Intelligence Information Reports (IIRs)).
- f. Provide targeting support and develop cyber targeting packages through all source intelligence on target systems, links, nodes, vulnerabilities, interdependencies, and others targets in support of current cyberspace operations.
- g. Develop products in conjunction with counterpart agency analysts or community wide efforts involving military service, Department of Defense (DoD), National, and international level intelligence elements.

- h. Research trends within an assigned subject-matter area and propose new or revised targeting projects to support collection.
- i. Develop and/or recommend innovative analytical approaches and solutions to problems and situations.
- j. Identify intelligence gaps and collection requirements to fill gaps and evaluate intelligence collected in response to requirements.

C.5.3.7 SUBTASK 7 – INTELLIGENCE SUPPORT TO REGIONAL CYBER CENTERS (RCCs)

The contractor shall provide all-source intelligence support for the RCCs. The contractor intelligence support shall include, but is not limited to, the following activities:

- a. Conduct all-source analysis and production support to full spectrum cyberspace operations and planning at the RCCs.
- b. Provide tailored, all-source current analysis addressing foreign and domestic Information Warfare and CNO capabilities, intentions, and actions affecting Army networks worldwide.
- c. Conduct research, analyze, and create products/reports from multiple intelligence and operational sources to provide situational awareness of critical elements of the cyberspace environment necessary to defend the network and DODIN.
- d. Remain aware of current activity trends of the organization's network and other Government and commercial networks.
- e. Contribute to the body of knowledge on foreign and domestic cyberspace capabilities and intentions.
- f. Assess threat modus-operandi, tools, techniques, alliances, and activities of hacker groups or cyber-related organizations and personnel within foreign governments, and of non-state actors such as terrorist groups.
- g. Support RM to track intelligence requirements and production efforts.
- h. Track and database all deliverables, RFIs, and tasking for the section.
- i. Respond to RFIs related to developing new assessments, distributing established assessments, or briefing new/established assessments about cyber threat capabilities and intentions.
- j. Fuse available intelligence with operational data into SIGINT, if applicable, and Collateral Daily/Weekly (INTSUMs).

C.5.3.8 SUBTASK 8 – SYSTEMS SUPPORT

The contractor shall provide technical support and training for applicable intelligence operations systems. Ancillary IT support is required under this subtask to support intelligence based systems. Support shall include, but is not limited to, the following activities:

- a. Provide onsite field support representative services to system users, including desk-side analytic training and expert assistance to analysts, and user account and system administration.
- b. Provide ancillary system support to include, but not limited to, software design, testing, development, and deployment for customer facing applications and application features.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- c. Document all application source code and functions (**Section F, Deliverable 3.3**), as required.
- d. Provide troubleshooting and bug fixes, and identify ways to optimize system performance.
- e. Collaborate with the engineering teams and ensure efficiency in code re-use and standardization.
- f. Implement security and data protection on applications, as applicable.
- g. Provide subject matter expertise on technology accreditation standards and procedures.
- h. Ancillary administration of operating systems (e.g., Red Hat Linux) to include command line interactions.
- i. Implement ontology changes to operations systems, as well provide weekly usage statistics, weekly health of software/hardware; manage user accounts, password resets, new account creation (e.g. Palantir Enterprise Manager).(Section F, Deliverable 3.4).
- j. Provide daily status checks of cron jobs (i.e., scheduled reports) that query, ingest, and transform new intelligence reporting into the repository.
- k. Ensure operating system and software remains Security Technical Implementation Guide (STIG) compliant with Information Assurance Vulnerability Alert (IAVA) patches.
- l. Analyze, troubleshoot, and/or report software or hardware faults to Government and third-party vendors.

C.5.3.9 SUBTASK 9 – INTELLIGENCE EXERCISES AND TRAINING

The contractor shall provide support for training and exercises. Contractor support shall include, but is not limited to, the following activities:

- a. Develop exercises to simultaneously assess and mitigate threats.
- b. Provide training management, scheduling, curriculum and materials for Active and Reserve Component Cyber Mission Force (CMF) (and non-CMF) training and exercises.
- c. Provide Training and Readiness Oversight (TRO).
- d. Provide support in the development of Master Scenario Events List (MSEL) and intelligence scenarios in support of exercises.
- e. Assist in conducting the exercise white cell.
- f. Conduct instruction on Intelligence Support in order for personnel to gain familiarization with the complex cyber environment, threats affecting Army Networks, and planning considerations.
- g. Provide Mobile Training Team (MTT) course to the service component, subordinate units, and requesting units. (Section F, Deliverable 3.5 and 3.6).
- h. Develop training surveys to solicit feedback on contractor-developed and contractor-led course modules (**Section F, Deliverable 3.7**), as required.
- i. Develop, update, and maintain course curriculum in accordance with Army Readiness Training (ART) policies (**Section F, Deliverable 3.6**) to include, but not limited to, the following:
 - 1. Real world current intelligence support to cyberspace operations.
 - 2. Army HUMINT/CI operations and activities in support of cyberspace operations.

3. Plan, coordinate, support, and deconflict intelligence planning support to cyberspace operations.
4. Coordinate, implement, and oversee intelligence policies, regulations, and directives with regards to cyberspace operations.
5. Conduct intelligence analysis of cyberspace threats using available intelligence tools.
6. Develop a working knowledge of the Intelligence Collection Planning Cycle in support of cyberspace operations.
7. Report writing in support of National, CCMD, and Service requirements (Cyber Threat Report (CTR), Automated Criminal Investigation Reporting System (ACIRs), and INTSUMs)
Identify, analyze, and implement training solutions designed to enhance ARCYBER operational intelligence capabilities.
- j. Disseminate, collect, and analyze the student self-assessment metrics to evaluate the data collected and identify emerging trends in students' learning experience. This data will be used to improve training initiatives, as needed
- k. Provide feedback and development capabilities on the application of simulation-based training in a synthetic environment.

C.5.4 TASK 4 – DEFENSIVE CYBERSPACE OPERATIONS (DCO)

ARCYBER HQ DCO plans, coordinates, integrates, synchronizes, directs, and conducts cyberspace operations in defense of all Army networks in order to maintain situational awareness and ensure timely and accurate C2 reporting. ARCYBER HQ DCO maintains Operational Control (OPCON) over the RCCs to include overseeing the defensive actions performed throughout the regions that are located in Southwest Asia, Europe, Hawaii, Korea, and Arizona. ARCYBER HQ DCO monitors and ingests information throughout the RCCs and facilitates information flow directly to the ARCYBER Commander.

The contractor shall assist in DCO planning, coordinating, integrating, synchronizing, and conducting cyberspace operations and defense of Army networks. The contractor shall develop and maintain SOPs and TTPs (**Section F, Deliverable 4.0**) pertinent to all DCO services, as required. The contractor shall develop a training program to ensure all personnel are trained and equipped to effectively perform their roles in DCO (**Section F, Deliverable 4.4 and 4.5**). The contractor shall develop reports and correspondence for the senior Military and Government leadership, as required (**Section F, Deliverable 0.1 and 0.3**).

C.5.4.1 SUBTASK 1 – INCIDENT MANAGEMENT (IM)

The IM team provides oversight of activities and is directly responsible for receiving, analyzing, and distributing information in order to mitigate cyber incidents/events occurring throughout the RCCs across the designated AORs. IM provides daily operational status briefings, makes technical recommendations, and provides procedural strategies for the Army Global “enterprise” network. IM provides technical support to the Army Cyber Operations Integration Center (ACOIC) staff during identification, resolution, and tracking of network intrusions and other cyber security incidents/events. IM coordinates with the RCCs, USCYBERCOM, JFHQ,

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

DODIN, LE/CI, and intelligence, and various other agencies in order to triage and systematically analyze cyber intrusion events.

The contractor shall assist in executing IM activities. Contractor support shall include, but is not limited to, the following activities:

- a. Provide a 24x7x365 IM capability.
- b. Provide technical expertise in support of cyberspace threat analysis.
- c. Manage cyber situational awareness portals and/or maintain a Cyber Common Operational Picture (CCOP).
- d. Conduct queries in incident databases on various issues such as trend analysis.
- e. Provide subject matter expertise on incidents to LE and CI agencies, as required
- f. Maintain an up-to-date POC list (**Section F, Deliverable 4.2**) for LE and CI agencies as routinely provided by Computer Crimes Investigative Unit (CCIU) and Cyber CI agencies.
- g. Track and monitor incident response activities (e.g., incident activities originating from a CSSP) throughout the lifecycle and report on metrics associated with the execution of the incident response lifecycle (**Section F, Deliverable 4.1 and 4.8**).
- h. Provide documentation through the appropriate channels on incidents and ensure standardization in documentation across the organization to DoD at large.
- i. Implement mitigation measures in response to general or Advanced Persistent Threats (APTs), attempted exploits/attacks, malware delivery, etc. on respective networks.
- j. Monitor incident response actions performed by the CSSP.
- k. Provide remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis, and direct system remediation tasks to on-site personnel.
- l. Prepare for, document, and maintain records of any required assessment of the execution of security operations (e.g., designated Cybersecurity Service Provider (CSSP) assessment) (**Section F, Deliverable 4.3**).
- m. Prepare detailed recommendations to the CSSP for network defense improvements to close or mitigate incidents on the DODIN.
- n. Prepare storyboard for ongoing operations (**Section F, Deliverable 4.9**), as required.
- o. Develop and publish incident response guidance and high-quality incident reports to appropriate audiences.
- p. Process, maintain, and provide receipt and tasking of tippers, NCTOC reports, and De-conflicting of reports for clarification.

C.5.4.2 SUBTASK 2 – ATTACK SENSING AND WARNING (AS&W)

The contractor shall provide detection, correlation, identification, and characterization of intentional unauthorized activity and coordinate information on detected events with required teams to ensure timely response is executed. The contractor shall provide support using scripting languages (e.g., Python, Perl, PowerShell, etc.) to understand the adversarial capabilities and risks. In addition, contractor support shall include, but is not limited to, the following activities:

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- a. Conduct global near real-time and historical analysis of network alerts/data using correlation tools and provide reports/TIPPERs to determine scope and internal defensive measures.
- b. Conduct open source research to identify commercial exploits or vulnerabilities (i.e., Zero-Day) requiring DCO actions.
- c. Develop correlation dashboards to identify events of interest.
- d. Identify current detection capabilities (e.g., Audio Visual (AV), Host Base Security System (HBSS), and Intrusion Detection System (IDS)/Intrusion Prevention Services (IPS)) for new or potential threat activity.
- e. Coordinate and develop host base and network base (IDS/IPS) signatures for implementation.
- f. Conduct initial troubleshooting of network sensor availability and coordinate with appropriate technicians to maintain sensor availability.
- g. Recommend refinements to user-defined signatures for network sensors to enhance overall effectiveness of sensor grid.
- h. Report and facilitate the correction of issues with correlation tools and data feed (**Section F, Deliverables 4.6 and 4.7**).
- i. Maintain, manage, and facilitate signature working group portal allowing for signature development and standardization for the enterprise.
- j. Maintain sensor location documentation for sensor grid layout and design.

C.5.4.3 SUBTASK 3 – CYBER RESPONSE TEAM

The contractor shall provide a cyber response team capability to develop mitigations in response to cyber threats. In addition, contractor support shall include, but is not limited to, the following activities:

- a. Track cyberspace effects requests and de-conflict with higher HQs, CCMDs, and other services and agencies.
- b. Track, review, identify, and submit pre-approved actions (i.e., IPblocks/Uniform Resource Locator (URL) blocks).
- c. Review, assess, and recommend mitigation actions in response to confirmed, potential threat activity, and unknown/new vulnerabilities.
- d. Prepare and brief pre-approved actions conducted, as required.
- e. Provide potential COAs, assessments, and technical expertise; and, enhance and improve the defensive posture, as required.
- f. Conduct vulnerability tests to identify operational impacts of activity directed against systems or applications.
- g. Update daily work logs with countermeasure details.
- h. Research and task network access exception requests (Whitelist).
- i. Research emerging best practice DCO and countermeasures.
- j. Publish and distribute reports related to cyber defense.

C.5.4.4 SUBTASK 4 – FORENSIC AND MALWARE ANALYSIS (F&MA)

The contractor shall provide digital media and network forensics using a variety of methods to detect and identify anomalous and/or malicious software. The contractor shall coordinate with internal and external mission partners to execute F&MA functions, including LE and CI liaison officers, and other intelligence professionals to understand higher-level adversary capability. The contractor shall analyze collected media to inform and improve defensive cyberspace capabilities and TTPs (**Section F, Deliverable 4.10**). In addition, contractor support shall include, but is not limited to, the following activities:

- a. Perform reverse-engineering on compiled executable code.
- b. Examine malicious software/capabilities to identify the nature of the threat.
- c. Reverse-engineer the compiled executable code to examine how the program interacts with its environment.
- d. Analyze collected media for DCO value to understand adversary technical capabilities and TTPs/methods of employment.
- e. Analyze the attack/exploit capability of the software, and document and catalog findings for future correlation.
- f. Develop and maintain malware analysis artifacts, reports, case notes, and all case related data, and ensure information is properly stored within the infrastructure (**Section F, Deliverable 4.11**). Provide all pertinent finding to personnel responsible for the development of signatures capable of detecting the analyzed malware as it propagates on infected systems.
- g. Perform dead-box forensic analysis and live forensic/incident handling analysis, as required, to include collection, preservation, and transfer forensic evidence of unauthorized access to a military/partner network, device, or Information Systems (IS); analyze forensically sound images to identify suspicious/malicious files, all intrusion related artifacts, and entry points/attack vectors; and develop necessary procedures or scripts to identify such data.
- h. Provide ancillary IT maintenance support for the forensic lab environment to include active directory (Windows), servers, (VMWare ESX), switches (CISCO/Brocade), and other network hardware/software appliances, as required.
- i. Update relevant portions of SOPs, TTPs, CSSP, website information, as required (**Section F, Deliverable 4.12**).

C.5.4.5 SUBTASK 5 – CYBER APPLICATIONS AND TOOLS

The contractor shall provide development and maintenance of cyber applications and tools. This includes infrastructure and application maintenance and upgrades, configuration management, system development (i.e., SDLC), and integration of existing tool sets to improve defensive cyber capabilities. Functional support under this subtask may be considered ancillary in accordance with the OASIS contract. In addition, contractor support shall include, but is not limited to, the following activities:

- a. Maintain and configure Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) and sensors; develop and test signatures; and document procedures

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- b. Update, maintain, configure security enterprise solutions (e.g., ArcSight Enterprise, etc.) to improve threat monitoring.
- c. Develop, maintain, and enhance cyber tools and software applications that improve tracking and facilitation of incident response.
- d. Develop dashboards, querying capabilities, trend analysis, and analysis tools using multiple data sources to correlate information.
- e. Identify and assess gaps in DCO capabilities and security posture and develop solutions as required.
- f. Develop and maintain documentation for activities as required.

C.5.5 TASK 5 – ENDPOINT SECURITY SYSTEM

The contractor shall provide planning, monitoring, reporting, and compliance of Endpoint Security (EPS) throughout the enterprise. The contractor shall perform all services during the core operational hours or as required per the shift assignments and threat priorities. The contractor may be required to adjust shift schedules and coverage in accordance with operational tempo. Contractor support shall include, but is not limited to, the following tasks:

- a. Assist in developing, reviewing, and modifying EPS guidance (e.g., Operations Order (OPORDs), Warning Orders (WARNORDs), Special Access Required (SAR), etc.).
- b. Develop, architect, and assist in overseeing the implementation of long-range projects related to EPS capabilities.
- c. Review and provide recommendations on the concurrence and non-concurrence of all exclusions and waivers.
- d. Maintain an internal collaboration and documentation portal (i.e., Sharepoint) for EPS activities.
- e. Provide subject matter expertise in the EPS product code and databases (e.g., McAfee Original Equipment Manufacturer (OEM) certified and employed personnel).
- f. Provide daily auditing of all ePolicy Orchestrator (ePO) servers for Secure Technical Implementation Guide (STIG) and ARCYBER required compliance.
- g. Perform configuration reviews of EPS documentation to include all network and system diagrams (Section F, Deliverable 5.3).
- h. Provide proactive threat detection and identify malicious activity across the Army Enterprise utilizing all EPS products and capabilities.
- i. Provide reports and briefings daily (Section F, Deliverable 5.2) on EPS compliance and threat related activity to senior military and civilian personnel.
- j. Coordinate and report threat activity in accordance with ARCYBER policies and procedures.
- k. Create and submit to ARCYBER personnel for approval and authorization to implement, EPS custom countermeasures to mitigate emerging threats.
- l. Review, analyze, and verify the current EPS configuration and effectiveness in response to emerging threats.
- m. Assess endpoints on the Army Enterprise network to meet DoD malware scanning and EPS compliance requirements.
- n. Provide support for the Army Enterprise standardization of ePO servers.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- o. Maintain and ensure ePO servers are configured, analyzed, monitored and adequately patched in accordance with applicable DoD Directives (DoDD).
- p. Maintain compliance with the standards required by Defense Information Systems Agency (DISA) Command Cyber Readiness Inspection (CCRI) in accordance with DISA and United States Sentencing Commission (USCC) guidelines.
- q. Provide STIG checklists and compliance reports (**Section F, Deliverables 5.5 and 5.6**).
- r. Provide Ports, Protocols, and Services Management (PPSM) information for customized or non-standard ports (**Section F, Deliverable 5.4**).

C.5.6 TASK 6 – INFORMATION ASSURANCE

The contractor shall provide 24x7x365 situational awareness and management of Army networks in support of HBSS, Assured Compliance Assessment Solution (ACAS), Information Assurance Vulnerability Management (IAVM), Cyber Scorecard, Vulnerability Disclosure Program, CCRI, and DODIN incidents. This includes real-time management and surveillance of the Army's portion of the DODIN. Contractor support shall include, but is not limited to, the following tasks:

- a. Perform vulnerability management and maintain cohesive coordination with USCC, JFHQ-DODIN, DISA, ARCYBER, Army Network Enterprise Technology Command (NETCOM), Command Duty Officer (CDO), RCCs, other agencies, and higher reporting echelons within the established timelines as established within the Commander's Critical Incident Requirements (CCIR)/Friendly Force Information Requirements (FFIR) reporting guide.
- b. Implement the IAVM and prepare weekly reports to assess progress (**Section F, Deliverable 6.1**).
- c. Track OPORDs (and other directives/requirements) issued by ARCYBER in order to improve compliance across the Army (**Section F, Deliverable 6.2**).
- d. Prepare and provide DODIN operational briefings to the ACOIC and provide input and subject matter expertise as required.
- e. Monitor, coordinate, and report network system and security incidents for the Army network infrastructure.
- f. Create and receive telephone and computer generated reports from Army IS, network elements, and users pertaining to status and operation of worldwide systems and facilities, both military and commercial, and identify and investigate the nature of technical difficulties involved.
- g. Coordinate with Theater Signal Commands, RCCs and other Cyber Operations Centers on outages and matters that require escalation to resolve technical deficiencies.
- h. Validate ACAS, CA Spectrum, and other web application reporting tools.
- i. Perform endpoint management and security scans using applicable tools (i.e., currently Tanium) to identify vulnerabilities across the DODIN (**Section F, Deliverable 6.0**).
- j. Review, analyze, track, and document incidents and outages and recommend de-confliction resolution and corrective measures. Prepare detailed briefs for senior leadership.

- k. Coordinate with the RCCs on Unauthorized Disclosures of Classified Information (UDCI) and other NetOps related issues to ensure adherence to proper procedures and guidelines.

C.5.7 TASK 7 – DODIN MISSION PLANNING

The contractor shall assist in planning, coordinating, and synchronizing DODIN Operations. The contractor shall architect, build, configure, secure, operate, maintain, and sustain networks and information. The contractor shall assist in operational planning and initiatives to support infrastructure and networks. The contractor shall support mission assurance efforts, to include the assessment and implementation of cybersecurity policies, programs, audits, accreditations, risk management, and maintenance of a cybersecurity scorecard.

C.5.7.1 SUBTASK 1 – PLANS AND INITIATIVES

Contractor support shall include, but is not limited to, the following tasks:

- a. Conduct network and infrastructure plans and assessments for the adoption and implementation of enterprise services, such as, cybersecurity, cloud computing services, Joint Information Environment, optical upgrades, Multi-Protocol Label Switching (MPLS), Joint Regional Security Stacks (JRSS), global ID, access management, and enterprise services (Section F, Deliverable 7.0).
- b. Provide weekly updates to the Commander's brief regarding the status of the implementation plans (Section F, Deliverable 7.1).
- c. Plan and assess Mission Partner Environment (MPE) to ensure security, standardization, and implementation of services and enable partner-nation capacity ISO theater security cooperation planning (Section F, Deliverable 7.2).
- d. Conduct tasks for DODIN operations missions received from higher HQs or mission partners (e.g., USCYBERCOM, JFHQ-DODIN, DISA, etc.).
- e. Assess the network environment and provide guidance for the operation and security of classified and unclassified network transport.
- f. Assist in assessing the enterprise network and infrastructure environment and developing plans for the adoption of new technologies that improve capabilities and security (Section F, Deliverable 7.3).

C.5.7.2 SUBTASK 2 – TECHNICAL ENGINEERING

Contractor support shall include, but is not limited to, the following tasks:

- a. Provide network and infrastructure subject matter expertise while assisting ARCYBER HQ in overseeing network and infrastructure implementation, optimization, consolidation, modernization, and cybersecurity efforts.
- b. Conduct daily synchronization and collaboration with strategic partners [e.g., JFHQ-DODIN, DISA, Command subordinate operations forces, Program Executive Office (PEOs) and others], as required.
- c. Develop operation plans (OPLANs) and OPORDs to implement infrastructure projects and support the documentation of all Army networks and connected devices and systems (Section F, Deliverable 7.4).

- d. Support the identification and defense of ARCYBER key terrain.
- e. Assist ARCYBER HQ in overseeing the implementation of network security to tactical edge.
- f. Evaluate select Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems for vulnerabilities, and recommend and implement remediation or migration.

C.5.7.3 SUBTASK 3 – MISSION ASSURANCE

Contractor support shall include, but is not limited to, the following tasks:

- a. Provide assistance in the development, inspection, evaluation, and oversight of cybersecurity policies and procedures.
- b. Review, evaluate, and maintain requirements to sustain enterprise certification and accreditation statuses (e.g. CSSP); recommend Measures of Effectiveness (MOEs) and Measures of Performance (MOPs); identify resource, policy, and technical gaps; and present recommendations on enterprise solutions to resolve technical and management gaps (**Section F, Deliverable 7.5**).
- c. Assist in reviewing written agreements (i.e., Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU)) between subscribers and providers to ensure compliance.
- d. Assist in preparing Army for inspections, such as, identifying and mitigating risks to using, processing, storing, and transmitting information or data.
- e. Review emerging policy, directives, standards, and technologies to determine implied and specified compliance actions and strategies; and, assist with the management of compliance data from all orders, alerts, and directives, including compiling reports to be presented, as required. Deliver final report following inspection (**Section F, Deliverable 7.7**).
- f. Plan, synchronize, assess, optimize, and employ endpoint protection and security solutions.
- g. Capture, perform quality assurance, and report/present, as required, a cumulative Scorecard report for the Secretary of Defense (SECDEF) and other Government officials (i.e., capturing data from systems such as ACAS and Enterprise Mission Assurance Support Service (eMASS)) (**Section F, Deliverable 7.7**).
- h. Conduct research on operational data and trend analysis to assist in planning, authoring, and tracking an enterprise improvement plan.

C.5.8 TASK 8 – PROTECTION PROGRAMS

C.5.8.1 SUBTASK 1 – CRITICAL INFRASTRUCTURE RISK MANAGEMENT (CIRM)

The contractor shall identify risks and vulnerabilities to critical infrastructure and ensure mitigations and remediation measures are implemented. Contractor support shall include, but is not limited to, the following tasks:

- a. Proactively identify CIRM-related issues.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- b. Develop and maintain CIRM-related policies and procedures (**Section F, Deliverable 0.8**).
- c. Develop draft briefings and provide meeting minutes in support of CIRM activities (Section F, Deliverables 0.2 and 0.3).
- d. Coordinate and synchronize assessment schedule, inspections, and risk mitigation strategies.
- e. Support critical asset and cyber vulnerability assessments (current estimates include 2-3 assessments per year at locations throughout CONUS, United States Northern Command (NORTHCOM), United States Southern Command (SOUTHCOM), United States Pacific Command (PACOM), United States European Command (EUCOM), and United States Central Command (CENTCOM)).
- f. Analyze functional assessments and proposed COA and recommend a COA to mitigate risks (Section F, Deliverable 8.2).
- g. Develop risk mitigation strategies and recommendations for identified vulnerabilities.
- h. Assess and identify critical assets (e.g., physical infrastructure, data/information, etc.) for the command and subordinate units and validate new critical asset requirements. Update applicable databases (e.g., Security Management Assessment Data (SMAD), etc.), as required (**Section F, Deliverable 8.1**).
- i. Analyze input from supporting organizations and other source agencies to draft a Risk Management Decision Package (RMDP) or prepare input to the supporting organization's RMDP (**Section F, Deliverable 8.0**).
- j. Assist in reviewing and contributing to holistic CIRM policy and procedures.
- k. Assist in updating Command's critical assets, as required.
- l. Track assessments (e.g., Joint Mission Analysis Assessments, etc.) and support all aspects of CIRM staff actions. Prepare and participate in all CIRM meetings and briefings.
- m. Review and participate in present and future on-site CIRM assessments and remediation working groups throughout the phased assessment process.
- n. Provide status reports for COAs associated with each RMDP at least monthly or more frequently as determined by the implementation schedule.

C.5.8.2 SUBTASK 2 – ANTITERRORISM (AT) AND FORCE PROTECTION (FP)

The contractor shall provide a broad range of technical and management support for AT and FP program efforts. The contractor shall provide qualified personnel with subject matter knowledge in AT and FP with completed ATO Training and certification (currently Level II and above). The contractor shall perform duties of a General Staff Action Officer/Command level AT Officer in accordance with designated regulations and policies (e.g., Army Regulation (AR) 525-13). Contractor support shall include, but is not limited to, the following tasks:

- a. Provide AT Plans Management support and coordination to the AT program.
- b. Develop and establish an AT program in accordance with Army standards. The AT program shall communicate the Command's intent of all AT policies supporting the pillars of protection and reducing vulnerabilities and mitigating threats from terrorist attacks.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- c. Create a system to collect, analyze, and disseminate terrorism threat information, and recommend the appropriate Army Force Protection Condition (FPCON) System.
- d. Serve as a member of a higher HQs assessment team and assess and reduce critical vulnerabilities (Conduct AT and supporting AT program assessments) (**Section F, Deliverable 8.4**).
- e. Provide strategic program planning support, analysis on mission trends and processes, and conduct and manage a robust assessment program.
- f. Assist in establishing terrorism threat/incident response planning, policies, and procedures that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents.
- g. Develop realistic terrorist threat scenarios and exercises that are relevant to the Army, Command, and its subordinates in accordance with Army standards.
- h. Provide assistance to coordinate, plan, and conduct the AT Training requirements, as required, in accordance with the AT Plan. Collaborate with physical security offices to ensure conference security requirements are met.
- i. Conduct training surveys and collect feedback to improve the quality of training.
- j. Develop, manage, and execute AT training and exercises in accordance with ARCYBER AT policy and training guidance as outlined in the AT Plan.
- k. Develop guidance, information papers, and procedures that modify security postures derived from the Army FPCON.
- l. Provide technical support to track and record assessment observations and tasking using SharePoint, Core Vulnerability Assessment Program (CVAMP), and/or Excel spreadsheets used to show AT mitigation strategies and/or response to its mission, to include responding to RFIs; staffing actions in the absence of the assigned staff officer or personnel; conducting training, when required; and reviewing and analyzing programs for content and effectiveness and resource functions of the Protection Division.
- m. Advise the Command of security deficiencies that would affect the security posture of units.
- n. Proactively identify CIRM-related issues.
- o. Develop AT policies and procedures in accordance with Army standards.
- p. Assist in researching and developing OPLANs and OPORDS (**Section F, Deliverable 8.3**).

C.5.9 TASK 9 – PLANNING, STRATEGY, POLICY, DOCTRINE, AND TECHNICAL SUPPORT

The contractor shall provide a broad range of research, programmatic, administrative, and resource support functions in support of organizational and mission planning, policy, doctrine, and technical support. In addition, contractor support shall include, but is not limited to, the following activities:

- a. Develop approaches to improve the organizational framework.
- b. Provide analysis of policies and regulations in support of various mission functions to include, but not limited to, IO, EW, and cyberspace operations.
- c. Perform duties as a staff action officer (**Section F, Deliverables 9.0-9.9**).

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- d. Support the Global Force Management (GFM) Process and Joint Operational Planning Process (JOPP) include, but not limited to, IO, EW, and cyberspace operations (**Section F, Deliverable 9.10**).
- e. Develop critical information products in programming and planning (**Section F, Deliverable 9.9**).
- f. Research and analyze doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) (**Section F, Deliverable 9.12**).
- g. Assist in refining the scope and characteristics of military operations in the cyberspace domain and analyze cyberspace doctrine, policy, and operating relationships within the greater cyberspace community.
- h. Support the development of plans for theater security cooperation requirements (**Section F, Deliverables 9.13-9.17**) in the cyberspace domain.
- i. Provide weekly and monthly status reports and executive summaries (**Section F, Deliverables 9.0**).
- j. Develop and incorporate new, revised, and improved business practices, processes, procedures, products, and strategies including supply chain management, using industry standard techniques (**Section F, Deliverable 9.11**) (e.g., Lean Six Sigma, Project Management Professional, etc.).

C.5.10 TASK 10 – READINESS TRAINING AND EXERCISES

The contractor shall assist in providing support for Joint and Army training, readiness, exercises, and modeling and simulation. This includes management of the Command training and exercise program, sustainable readiness, and modeling and simulation actions within cyber operations, EW, and IO in order to enhance operational readiness and TRO in the cyberspace domain for Cyber Electromagnetic Activity (CEMA) (AR 10-87). The contractor shall:

- a. Assist in coordination and execution of training and education for the Command training, readiness, exercises, and modeling and simulation programs, the CMF, IO, and EW units for sustainable readiness, exercises, and mission rehearsals (**Section F, Deliverables 10.0 and 10.2**).
- b. Assist with management, seat allocation, and Program Objective Memorandum (POM) build for CMF individual and collective 1000 thru 4000 level training for the Army.
- c. Assist with management for latest Microsoft (MS) Windows certification training for the Army.
- d. Assist in planning, support, and management of TRO for Cyberspace Operations, IO, and EW units in the active and reserve component units (**Section F, Deliverable 10.5**).
- e. Assist in planning and management of the sustainable readiness program (**Section F, Deliverable 10.6**).
- f. Assist in developing policies and plans and for training, readiness, exercises, and modeling and simulation of Army forces in the cyberspace domain for CEMA to include CENTROPY and training management databases (**Section F, Deliverable 10.4**).
- g. Provide subject matter expertise on means for training, readiness, exercises, and modeling and simulation individuals and units for CEMA.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- h. Assist with monitoring readiness of training, readiness, exercises, and modeling and simulation facilities to assess adequacy of training means in CEMA (**Section F, Deliverable 10.3**).
- i. Support the collection, analysis, and dissemination of readiness reporting requirements and Mission Essential Task (MET) development in CEMA (**Section F, Deliverable 10.1**).
- j. Provide research and analyses to assist ARCYBER in effective exercise development and execution in CEMA.
- k. Assist in developing cyberspace operational and planning concepts and evaluating the Command's ability to support real-world operations.
- l. Assist in planning, researching, and developing training, readiness, exercises, and modeling and simulation programs that more effectively deal with rapid changes in the cyberspace domain and resulting CEMA mission sets.
- m. Assist in supporting the ARCYBER Cyber Professional Development (CPD) Program training, education, experience events, and opportunities.
- n. Assist in developing/updating learning objectives using Command training concepts (e.g., Objective and Pillars) (**Section F, Deliverable 10.2**).
- o. Assist in establishing a lessons learned policy and process (**Section F, Deliverable 10.4**).

C.5.11 TASK 11 – INFORMATION OPERATIONS (IO)

The contractor shall provide a broad range of activities that support the development and integration of IO, EW, Space, and Special Technical Operations (STO) into cyberspace mission, strategy, plans, and operations. Contractor support shall include, but is not limited to, the following activities:

- a. Review policies and develop plans (i.e., Concept of Operations (CONOPS), OPLANs, and Contingency Plans), doctrine, and policies (**Section F, Deliverable 11.2**).
- b. Develop, coordinate, and implement Operations Security (OPSEC) into activities and operations and provide recommended mitigations.
- c. Produce information and decision papers, executive summaries, weekly activity reports, and operational briefs (**Section F, Deliverable 11.0; 11.3**).
- d. Collect, compile, analyze, and report on IO programs and activities.
- e. Provide knowledge management capabilities in support of IO.
- f. Support the development and maintenance of SOPs.
- g. Monitor, track, and coordinate IO training requirements.
- h. Assist with the development of OPSEC assessments, surveys, long-range plans, goals, and milestones. (**Section F, Deliverable 11.4**)
- i. Provide support to STO programs including, but not limited to: SAP, SAR, and Common Access Billets (CAB) programs.
- j. Provide recommendations for capabilities in support of IO (e.g., EW equipment, etc.).
- k. Develop target nomination packets (**Section F, Deliverable 11.6**)
- l. Assist in conducting crisis action planning and participating in B2C2WGs.
- m. Participate in quarterly IO summits or as required (**Section F, Deliverable 11.1**).

C.5.12 TASK 12 – COMMUNICATIONS SUPPORT

The contractor shall provide assistance in the development and maintenance of the Command's communication materials, public information, and community relations/outreach that inform and educate internal and external audiences about Command activities, capabilities, goals, and priorities. In addition, contractor support shall include, but is not limited to, the following activities:

- a. Plan, design, develop, and maintain internal and external public websites and social media platforms, including the integration of embedded videos, live tiles, and emerging trends in technology.
- b. Assist in the design and implementation of new technology to support the Command's information objectives (e.g., mobile applications, etc.).
- c. Provide technical writing and editing support for Command and public information publications (**Section F, Deliverable 12.6**).
- d. Develop Command and public information materials for publication (e.g., magazines, brochures, mailers, etc.)
- e. Leverage analytics to improve the user experience and optimize performance of websites (**Section F, Deliverable 12.5**).
- f. Design and develop a variety of graphics to support Command and public information (e.g., logos, posters, pamphlets, animation, three dimensional effects, etc.) (**Section F, Deliverables 12.1 and 12.2**).
- g. Ensure websites are compliant with all applicable DoD standards and policies (e.g., Section 508 accessibility and privacy act, etc.) and appropriate security standards are met (**Section F, Deliverable 12.0**).
- h. Develop and present briefings to senior military and civilian personnel (**Section F, Deliverable 12.4**).
- i. Develop and maintain SOPs for all applicable activities (**Section F, Deliverable 12.3**).

C.5.13 TASK 13 – FORCE DEVELOPMENT

The contractor shall provide a broad range of research, programmatic, and administrative functions in support of programming, capabilities integration, organizational design, and force integration. The contractor shall perform all services during the core operational hours or as required per the evolving priorities. In addition, this support includes, but is not limited to, the following activities:

- a. Conduct research to provide analysis of and input to Army Force Management processes, including Total Army Analysis (TAA), Command Plan, and POM with minimal supervision.
- b. Conduct research and analysis on DOTMLPF-P.
- c. Provide input and facilitate the staffing and/or processing of Concept Plans and Force Design Updates.
- d. Provide support to the command plan process to include, but not limited to, analyzing plans, drafting OPORDs, conducting In-Process Reviews (IPRs), and preparing Schedule 8 submissions, etc.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- e. Assist in the development of Force Management products (e.g., Concept Plans, Cost Benefit Analysis, Tables of Distribution and Allowances (TDAs), and manpower studies).
- f. Provide support to the Requirements and Oversight Council Process (e.g., Joint Capability Integration and Development System (JCIDS) document reviews in support of system survivability).
- g. Support the commands capability gap assessment process, capability development, and integration (e.g., Joint Urgent Operational Need (JUON), Joint Emerging Operational Need (JEON) requirements documents, etc.).
- h. Provide Force Integration support including, but not limited to, new equipment fielding and new equipment training.
- i. Provide expert cost-benefit analysis for proposed IO and cyber requirements and courses of action to enable senior leaders to make resource informed decisions (**Section F, Deliverable 13.1**).
- j. Schedule rooms and video teleconferencing sessions, maintain contact lists, and disseminate notifications, agendas, and read-ahead packages for all meetings and conferences.
- k. Draft and provide briefings, information/decision papers, policy documents, staffing packages, letters, memorandums, and official multimedia correspondence (**Section F, Deliverable 13.2**).
- l. Provide organizational change management support of functional reviews and manpower studies to include, but not limited to, developing study frameworks and methodologies, conducting research and analysis, interviewing subjects, identifying gaps, seems, and redundancies, and developing recommendations based on both qualitative and quantitative data.

C.5.14 TASK 14 – CYBER MISSION PARTNER SUPPORT (OPTIONAL)

Establishing a Cyber Mission Partner Support function under this TO will advance collaboration, research, information sharing, strategy, and best practices between ARCYBER, its subordinate components, service component partners of CYBERCOM, and other DOD cyber mission partners. This includes the organizations depicted as a part of the Army Cyberspace C2 Framework referenced in Section J, Attachment T.

This task area shall provide the full scope of cyberspace capabilities as defined in tasks 1 through 13 in support of short to long term, as-needed requirements. The contractor shall work directly with mission partner stakeholders to ingest requirements documentation and develop and execute plans that rapidly deploy cyber resources and capabilities to the mission partner environment. The contractor shall produce custom deliverables, reports, and other products in accordance with mission partner stakeholder requirements.

In addition to tasks 1 through 13, this scope may include, but is not limited to, the following activities:

- a. Assist with the research and development of cyberspace capabilities to include, but not limited to, artificial intelligence, ICSs, cyber weapon systems, war games, and other cutting edge capabilities.

SECTION C – DESCRIPTION / SPECIFICATIONS / PERFORMANCE WORK
STATEMENT

- b. Develop, test, and integrate defensive and offensive cyber capabilities and solutions to protect critical infrastructure and assets and disrupt and neutralize the adversary's.
- c. Provide "On Call" response teams to rapidly respond to cyber threats.
- d. Identify, recommend, and develop solutions to synchronize and standardize global mission partner operations.
- e. Plan and conduct the full range (i.e., strategic, tactical, and operational) of cyber flag exercises and cyber training support, as required.
- f. IO training to include Cyber Operations Training, Network Traffic Analysis, Cyber Threats Detection and Mitigation, Malicious Network Traffic Analysis, CNO, Computer Network Exploitation, and CNO Attack and Defend.